ABSTRACT

A smart card and a settlement terminal are provided by which, when common-key cryptography is used for value transfer between smart cards, the security of the whole system can be improved by enabling easy updating of a cryptographic key used for the value transfer. A smart card transmits/receives value data to/from another smart card. The smart card includes an information accumulating unit for accumulating value data, a transfer key used to update the value data, and an update key used to update the transfer key; a communication unit for receiving a transfer key encrypted by use of the update key, the transfer key being transmitted from another smart card; and an arithmetic processing unit for decrypting the encrypted transfer key by use of the update key to update the transfer key accumulated in the information accumulating unit by use of the decrypted transfer key.